Kerberos V, OpenLDAP, OpenAFS

Using Debian GNU/Linux

Dr. Wolfgang A. Gehrke

wgehrke@dia.uniroma3.it

Dipartimento di Informatica e Automazione
Università degli Studi Roma Tre

Overview

Overview

- short site report

Overview

- short site report
- our motivation for alternative cell

Overview

- short site report
- our motivation for alternative cell
- core architecture =
  Kerberos V + OpenLDAP + OpenAFS

Overview

- short site report
- our motivation for alternative cell
- core architecture =
  Kerberos V + OpenLDAP + OpenAFS
- benefits of this core

Overview

- short site report
- our motivation for alternative cell
- core architecture =
  Kerberos V + OpenLDAP + OpenAFS
- benefits of this core
- implementation with Debian

Overview

- short site report
- our motivation for alternative cell
- core architecture =
  Kerberos V + OpenLDAP + OpenAFS
- benefits of this core
- implementation with Debian
- application scenarios

Overview

- short site report
- our motivation for alternative cell
- core architecture =
  Kerberos V + OpenLDAP + OpenAFS
- benefits of this core
- implementation with Debian
- application scenarios
- gained experience

Overview

- short site report
- our motivation for alternative cell
- core architecture =
  Kerberos V + OpenLDAP + OpenAFS
- benefits of this core
- implementation with Debian
- application scenarios
- gained experience
- next steps

Site Report

current cell vn.uniroma3.it for $\geq$ 10 years

alternative cell dia.uniroma3.it for $\approx$ 2 years

servers Dell PowerEdge SCSI HW RAID5

clients (AIX), Linux, MacOS X, (Windows XP)

volumes many backups, few replicas, some copies

backups to file on hard disk

users students, lecturer, staff

conventional use homes, mail, web

advanced use computer based exams, lab software

useful new commands found in OpenAFS

Context

department
: part of Engineering from our university

hardware
: 32bit Intel off-the-shelf

software
: mainly open source, Windows Campus licence

Linux distributions
: Debian, Gentoo, Ubuntu

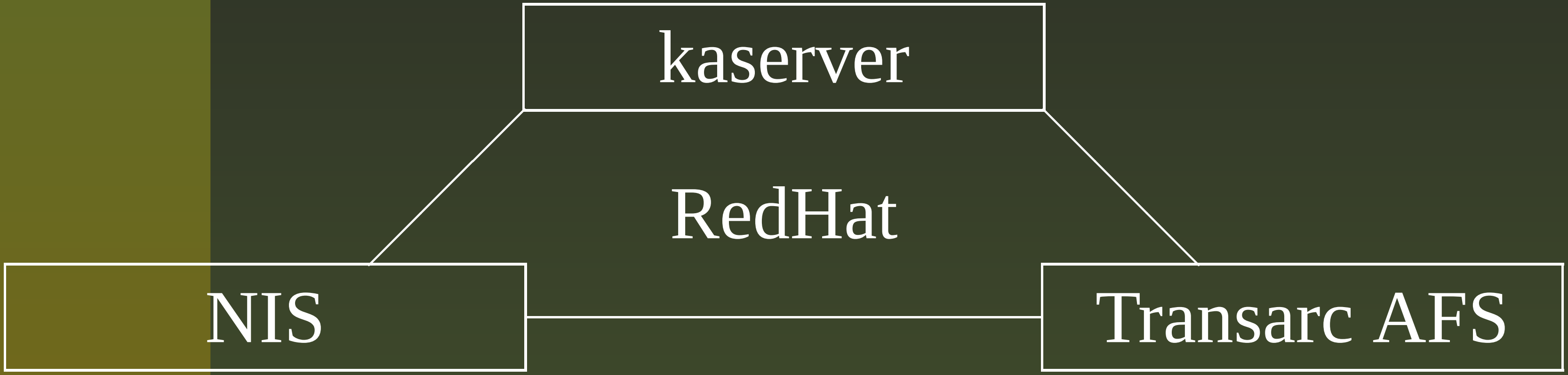
advancing technologies
: parallel, distributed, grid computing;
new Windows 2000 server architecture

Motivation for alternative Cell

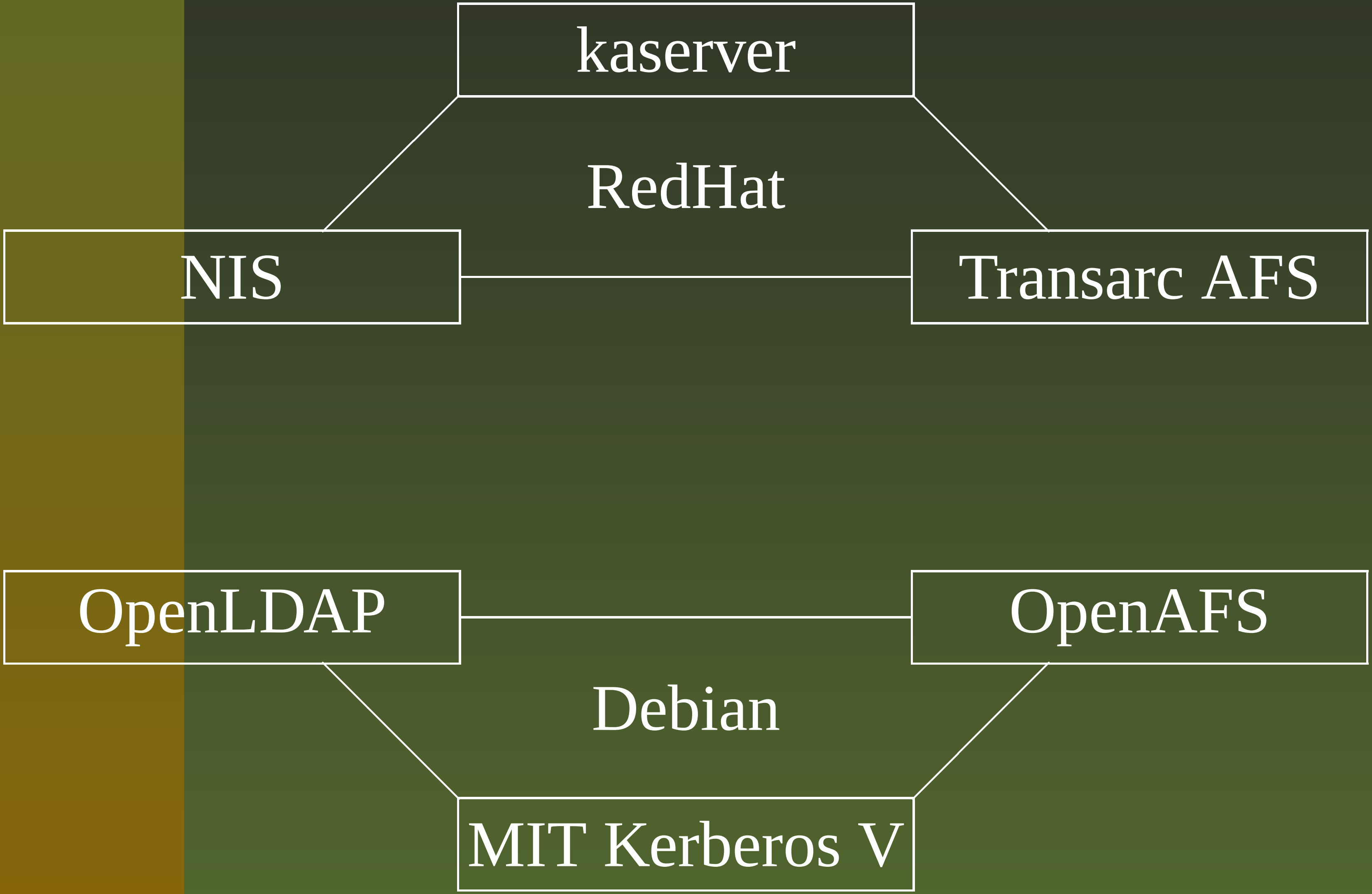
1. cell vn.uniroma3.it with external support
2. customized RedHat Linux
3. started with Transarc and now OpenAFS
4. on “AS IS” blackbox basis
5. born during the period of many UNIX dialects
6. no direct access to AFS administrative commands
7. kaserver (now fakeka) + NIS based
8. local mail spool but UW-imap folders in AFS
9. some ACLs with IPs but no keytabs

Core Architecture Shift

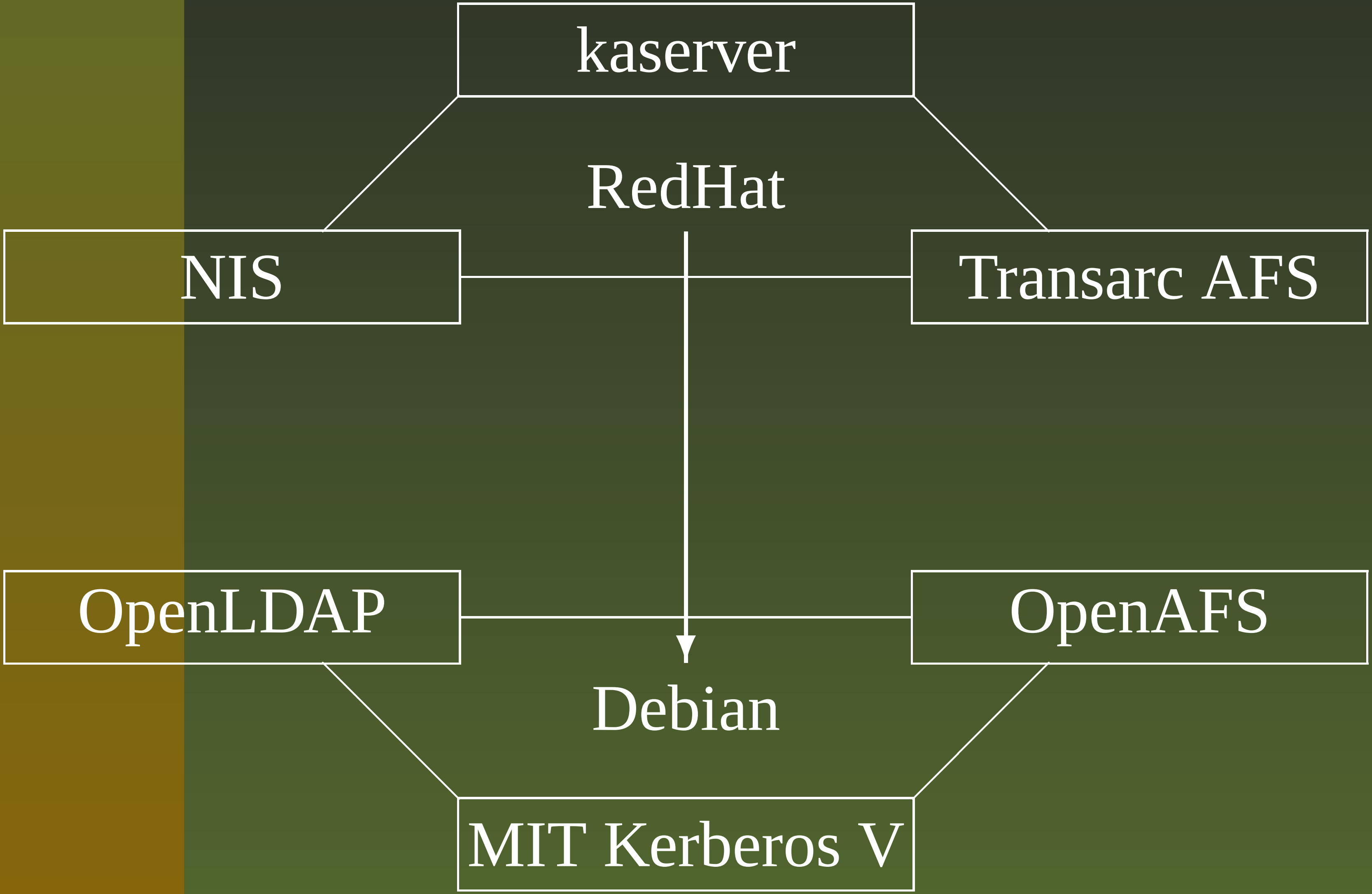
Core Architecture Shift



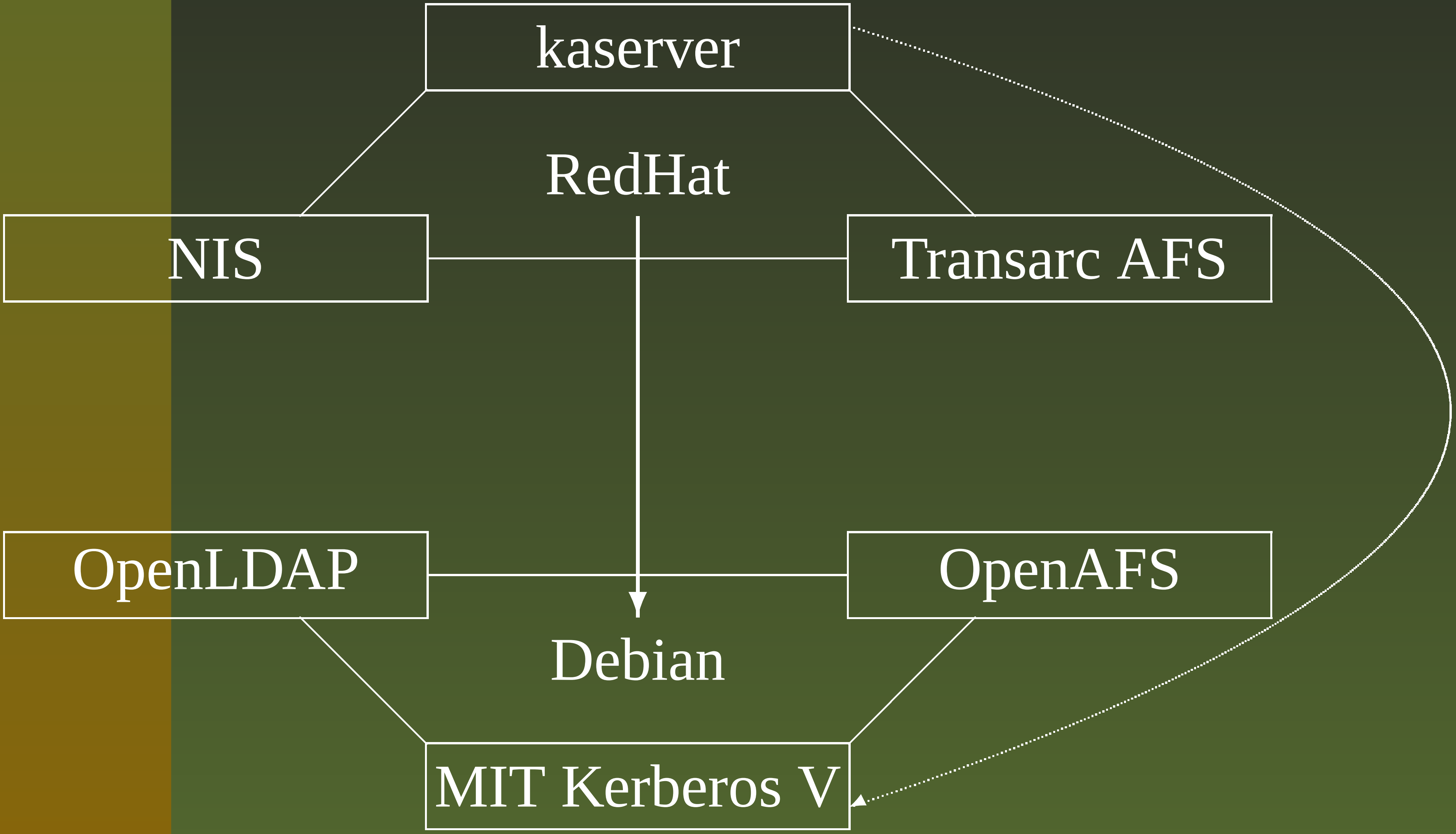
Core Architecture Shift



Core Architecture Shift



Core Architecture Shift


kaserver

RedHat

NIS

Transarc AFS

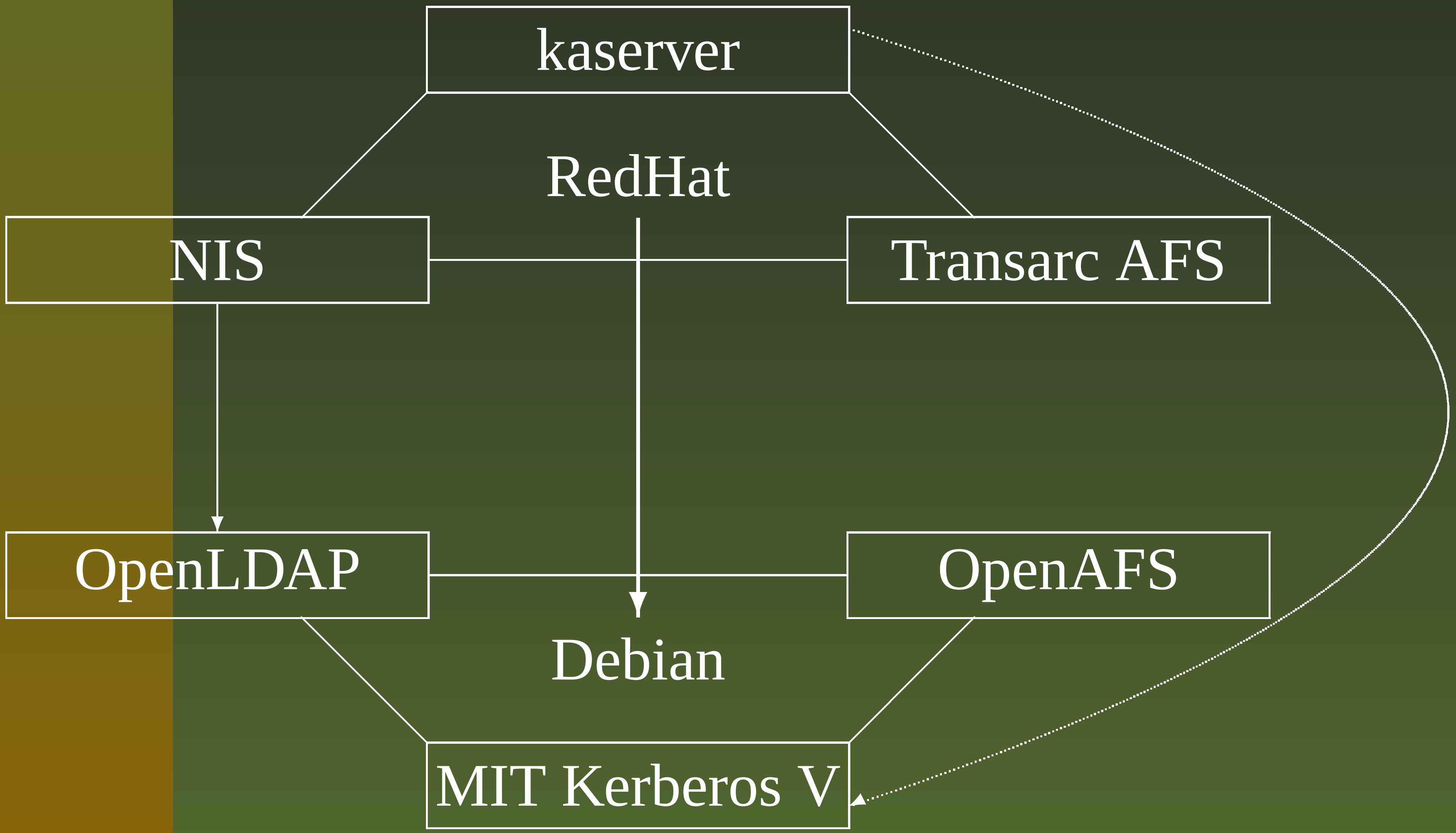
OpenLDAP

OpenAFS

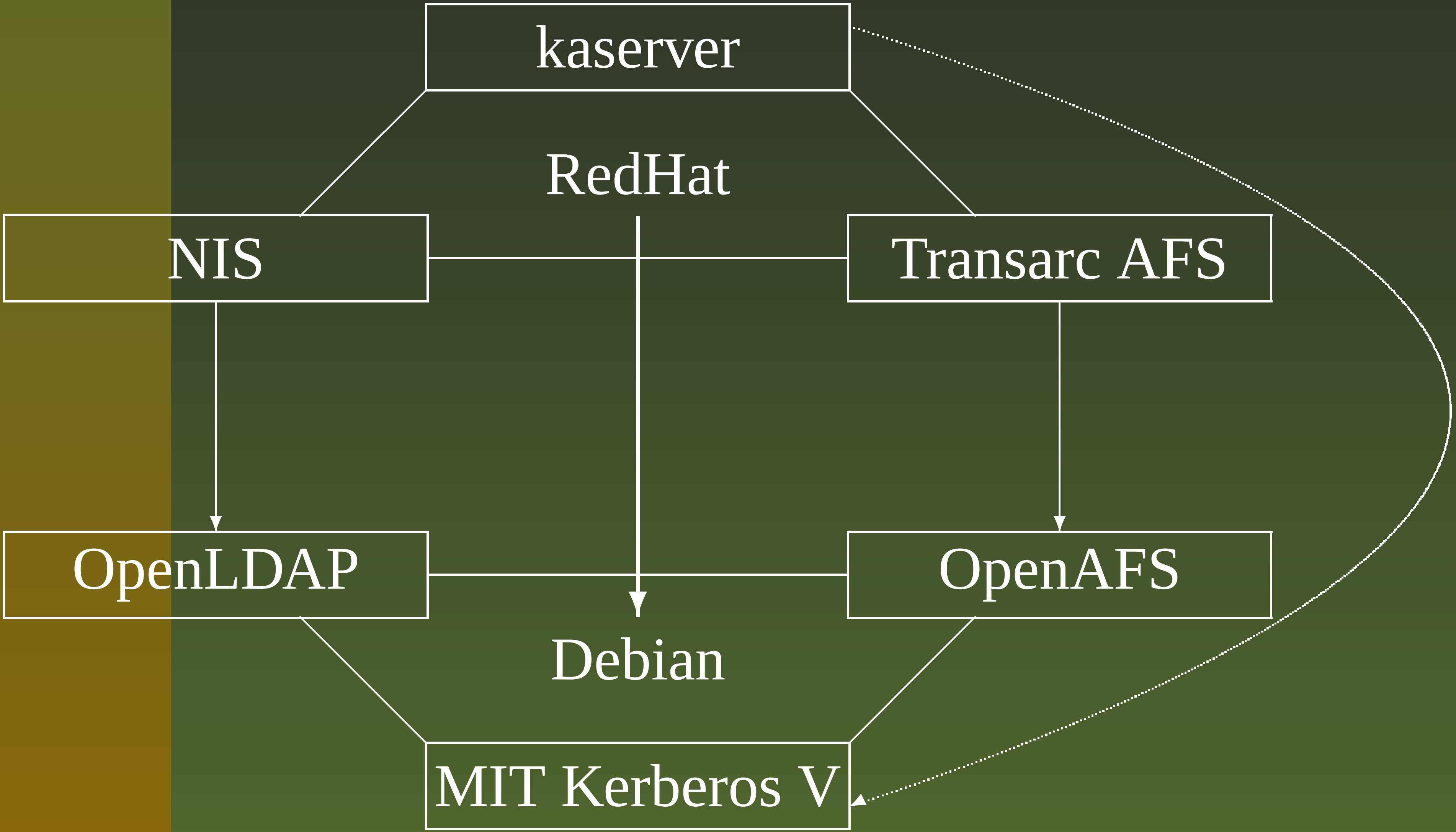
Debian

MIT Kerberos V

Core Architecture Shift



Core Architecture Shift



Benefits of this Core

Benefits of this Core

KRB5: centralized authentication

- master and slave
- PAM module

Benefits of this Core

KRB5: centralized authentication

- master and slave
- PAM module

LDAP: centralized information

- replication
- SASL with GSSAPI

Benefits of this Core

KRB5: centralized authentication

- master and slave
- PAM module

LDAP: centralized information

- replication
- SASL with GSSAPI

OpenAFS: distributed filesystem

- redundancy
- allows for mail and web integration
- low-cost NAS/SAN substitution over Ethernet

Implementation with Debian

Implementation with Debian

MIT Kerberos V+OpenLDAP+OpenAFS: out of the box

Implementation with Debian

MIT Kerberos V+OpenLDAP+OpenAFS: out of the box

	apache2	postfix-tls	courier-imap-ssl
KRB5			
LDAP			
oAFS			

Implementation with Debian

MIT Kerberos V+OpenLDAP+OpenAFS: out of the box

	apache2	postfix-tls	courier-imap-ssl
KRB5	mod-auth-kerb	saslauthd	courierauthd
	keytab	PAM	PAM
LDAP	UserDir	aliases	HOME
oAFS	mod_dav	procmail	MAILDIR
	DAV access	MAILDIR	access

Implementation with Debian

MIT Kerberos V+OpenLDAP+OpenAFS: out of the box

	apache2	postfix-tls	courier-imap-ssl
KRB5	mod-auth-kerb keytab	saslauthd PAM	courierauthd PAM
LDAP	UserDir	aliases	HOME
oAFS	mod_dav DAV access	procmail MAILDIR	MAILDIR access

	ssh	inn2	postgresql
KRB5			
LDAP			
oAFS			

Implementation with Debian

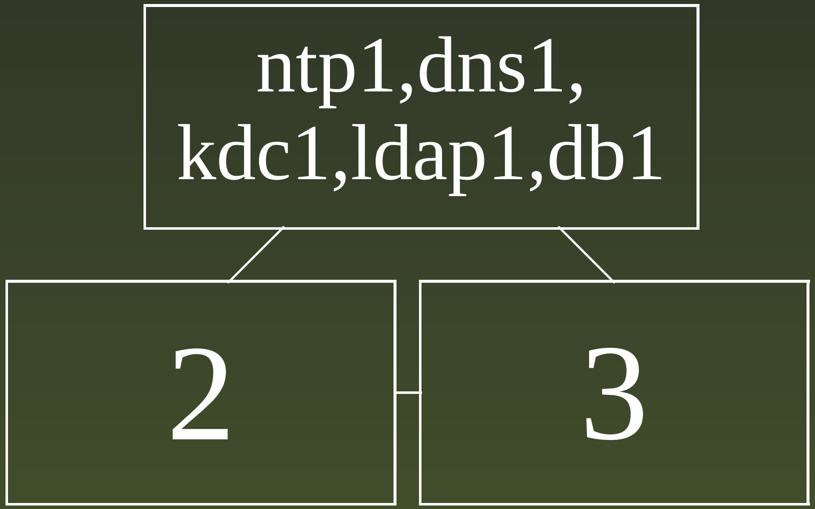
MIT Kerberos V+OpenLDAP+OpenAFS: out of the box

	apache2	postfix-tls	courier-imap-ssl
KRB5	mod-auth-kerb keytab	saslauthd PAM	courierauthd PAM
LDAP	UserDir	aliases	HOME
oAFS	mod_dav DAV access	procmail MAILDIR	MAILDIR access

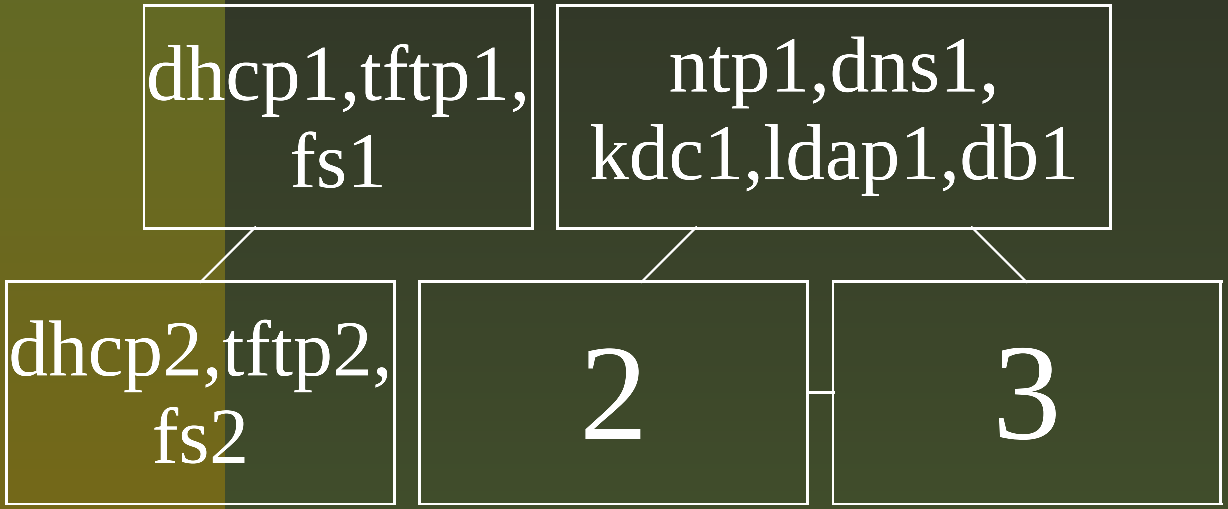
	ssh	inn2	postgresql
KRB5	GSSAPI + PAM	RADIUS + PAM	keytab
LDAP	NSS		
oAFS	HOME	(spool)	(backup)

Redundancy

Redundancy



Redundancy


dhcp1,tftp1, fs1

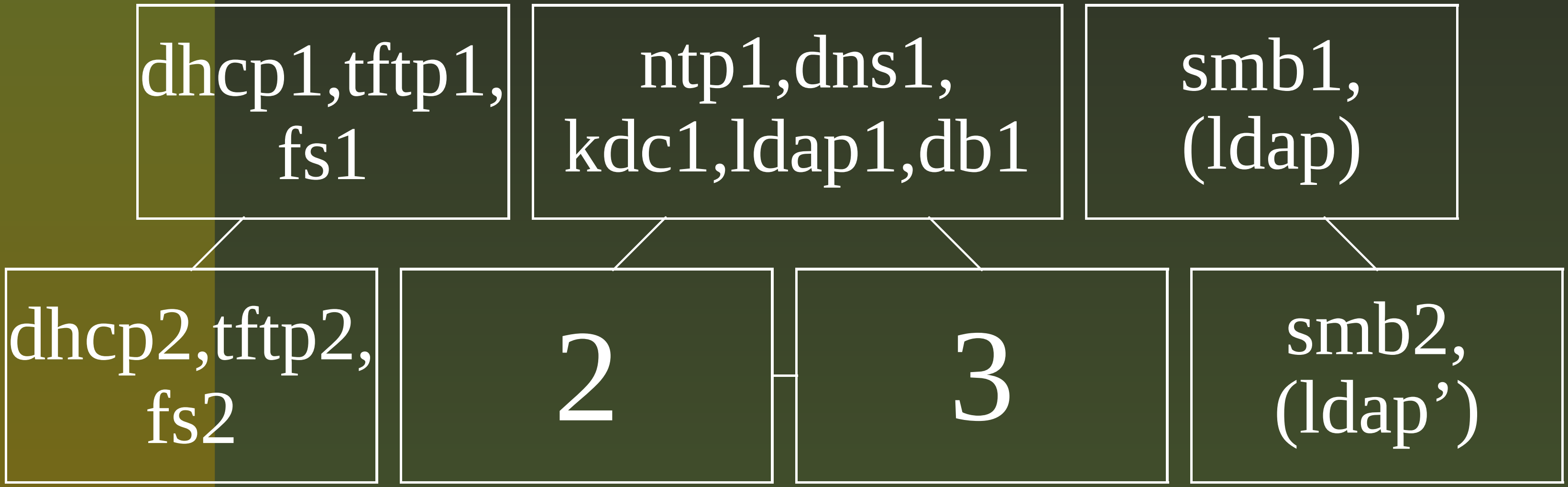
ntp1,dns1, kdc1,ldap1,db1

dhcp2,tftp2, fs2

2

3

Redundancy



dhcp1,tftp1, fs1

ntp1,dns1, kdc1,ldap1,db1

smb1, (ldap)

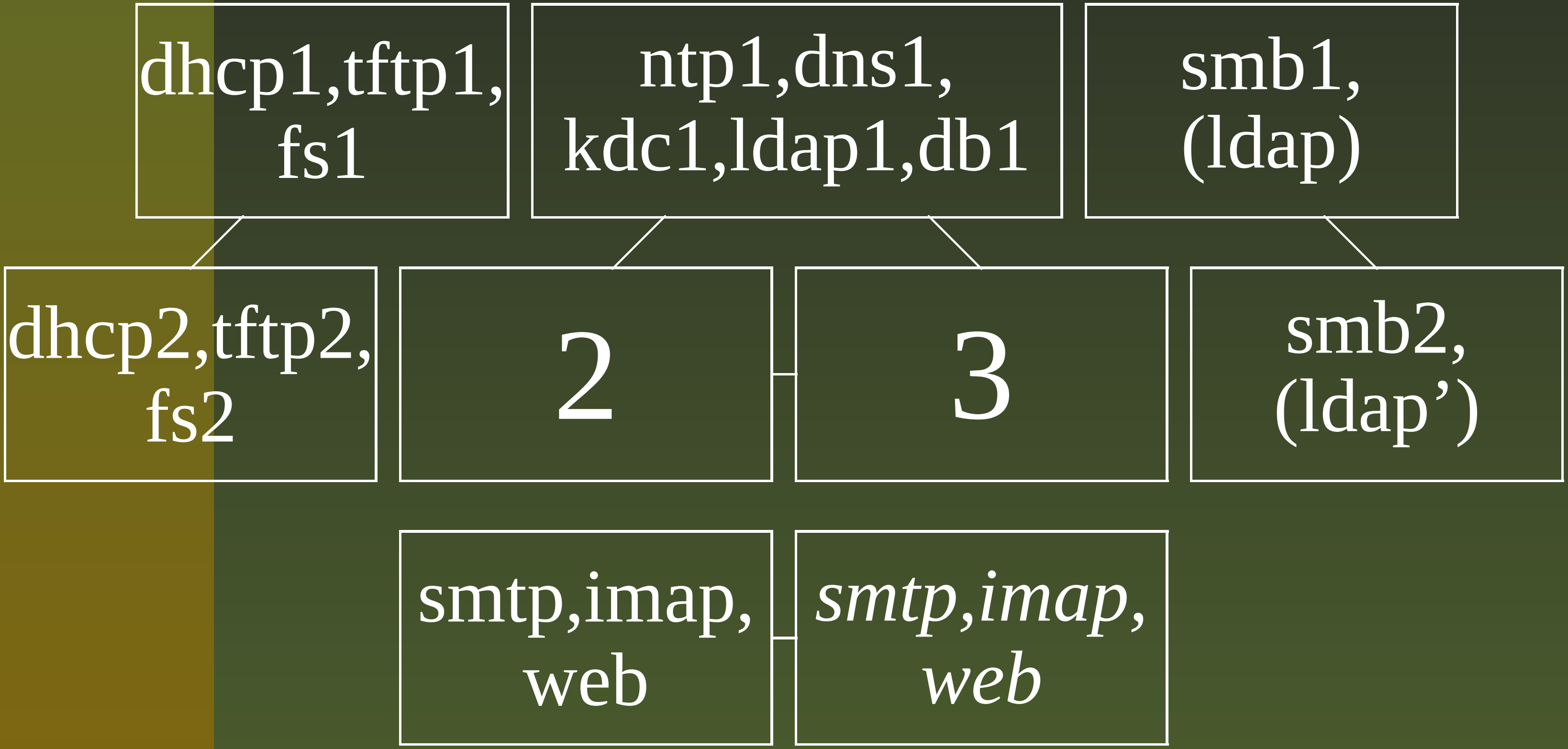
dhcp2,tftp2, fs2

2

3

smb2, (ldap’)

Redundancy



dhcp1,tftp1,
fs1

ntp1,dns1,
kdc1,ldap1,db1

smb1,
(ldap)

dhcp2,tftp2,
fs2

2

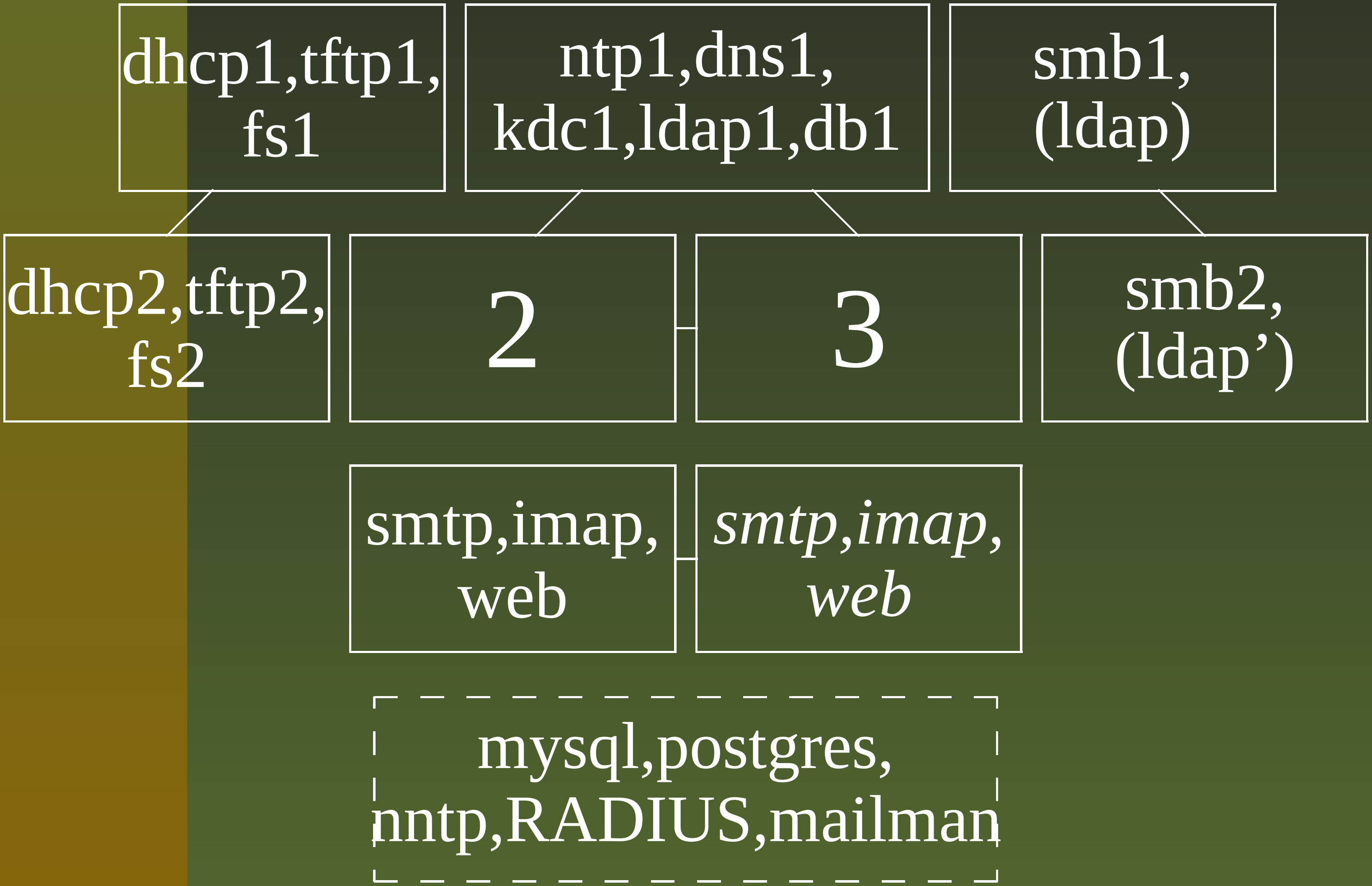
3

smb2,
(ldap')

smtp,imap,
web

smtp,imap,
web

Redundancy



dhcp1,tftp1, fs1

ntp1,dns1, kdc1,ldap1,db1

smb1, (ldap)

dhcp2,tftp2, fs2

2

3

smb2, (ldap’)

smtp,imap, web

smtp,imap, web

mysql,postgres, nntp,RADIUS,mailman

Computer Based Exams

Computer Based Exams

1. rc.local in AFS space
   - kiosk mode
   - permits firewall activation

Computer Based Exams

1. rc.local in AFS space
   - kiosk mode
   - permits firewall activation
2. generic user on lab computer with IP based ACL
   - symbolic link into IP enabled work space
   - similar to possible NFS setting

Computer Based Exams

1. rc.local in AFS space
   - kiosk mode
   - permits firewall activation
2. generic user on lab computer with IP based ACL
   - symbolic link into IP enabled work space
   - similar to possible NFS setting
3. home volume replacement
   - for specialized exams
   - prepare fresh empty volume
   - set real home volume offline during exam

Administration Tools with PROLOG

Administration Tools with PROLOG

- scope: static analysis + basic operations
  (not full-blown ADM server)

Administration Tools with PROLOG

- scope: static analysis + basic operations (not full-blown ADM server)
- need consistency between data bases for Kerberos, LDAP, and pts

Administration Tools with PROLOG

- scope: static analysis + basic operations
  (not full-blown ADM server)
- need consistency between data bases
  for Kerberos, LDAP, and pts
- simple db extraction to file in Prolog syntax

Administration Tools with PROLOG

- scope: static analysis + basic operations (not full-blown ADM server)
- need consistency between data bases for Kerberos, LDAP, and pts
- simple db extraction to file in Prolog syntax
- this file gets just loaded into Prolog

Administration Tools with PROLOG

- scope: static analysis + basic operations
  (not full-blown ADM server)
- need consistency between data bases
  for Kerberos, LDAP, and pts
- simple db extraction to file in Prolog syntax
- this file gets just loaded into Prolog
- consistency easy to express with logic programming

Administration Tools with PROLOG

- scope: static analysis + basic operations (not full-blown ADM server)
- need consistency between data bases for Kerberos, LDAP, and pts
- simple db extraction to file in Prolog syntax
- this file gets just loaded into Prolog
- consistency easy to express with logic programming
- backtracking suitable for “undo” operation

Administration Tools with PROLOG

- scope: static analysis + basic operations (not full-blown ADM server)
- need consistency between data bases for Kerberos, LDAP, and pts
- simple db extraction to file in Prolog syntax
- this file gets just loaded into Prolog
- consistency easy to express with logic programming
- backtracking suitable for “undo” operation
- need to extend initial scripts

Further Gained Experience

Further Gained Experience

- secure services require SSL/TLS

Further Gained Experience

- secure services require SSL/TLS
- implementation of a small in-house PKI

Further Gained Experience

- secure services require SSL/TLS
- implementation of a small in-house PKI
- mainly for private host keys and certificates

Further Gained Experience

- secure services require SSL/TLS
- implementation of a small in-house PKI
- mainly for private host keys and certificates
- user certificates can be published in LDAP

Further Gained Experience

- secure services require SSL/TLS
- implementation of a small in-house PKI
- mainly for private host keys and certificates
- user certificates can be published in LDAP
- users can benefit from e.g. USB tokens (smartcards)

Further Gained Experience

- secure services require SSL/TLS
- implementation of a small in-house PKI
- mainly for private host keys and certificates
- user certificates can be published in LDAP
- users can benefit from e.g. USB tokens (smartcards)
- possibilities:

  - certificate based mail relay
  - certificate based web access
  - mail signing and encryption

Next Steps

Next Steps

1. adding firewall rules (DDOS)

Next Steps

1. adding firewall rules (DDOS)
2. server hardening (SELinux)

Next Steps

1. adding firewall rules (DDOS)
2. server hardening (SELinux)
3. Ubuntu on server

Next Steps

1. adding firewall rules (DDOS)
2. server hardening (SELinux)
3. Ubuntu on server

... AND ...

2007 book by Springer with Ing. Franco Milicchio
“Distributed Services with OpenAFS
for Enterprise and Education”

Next Steps

1. adding firewall rules (DDOS)
2. server hardening (SELinux)
3. Ubuntu on server

... AND ...
2007 book by Springer with Ing. Franco Milicchio
“Distributed Services with OpenAFS
for Enterprise and Education”

PLUS: help wanted for AIX
(5.2 on a donated pSeries for CATIA)